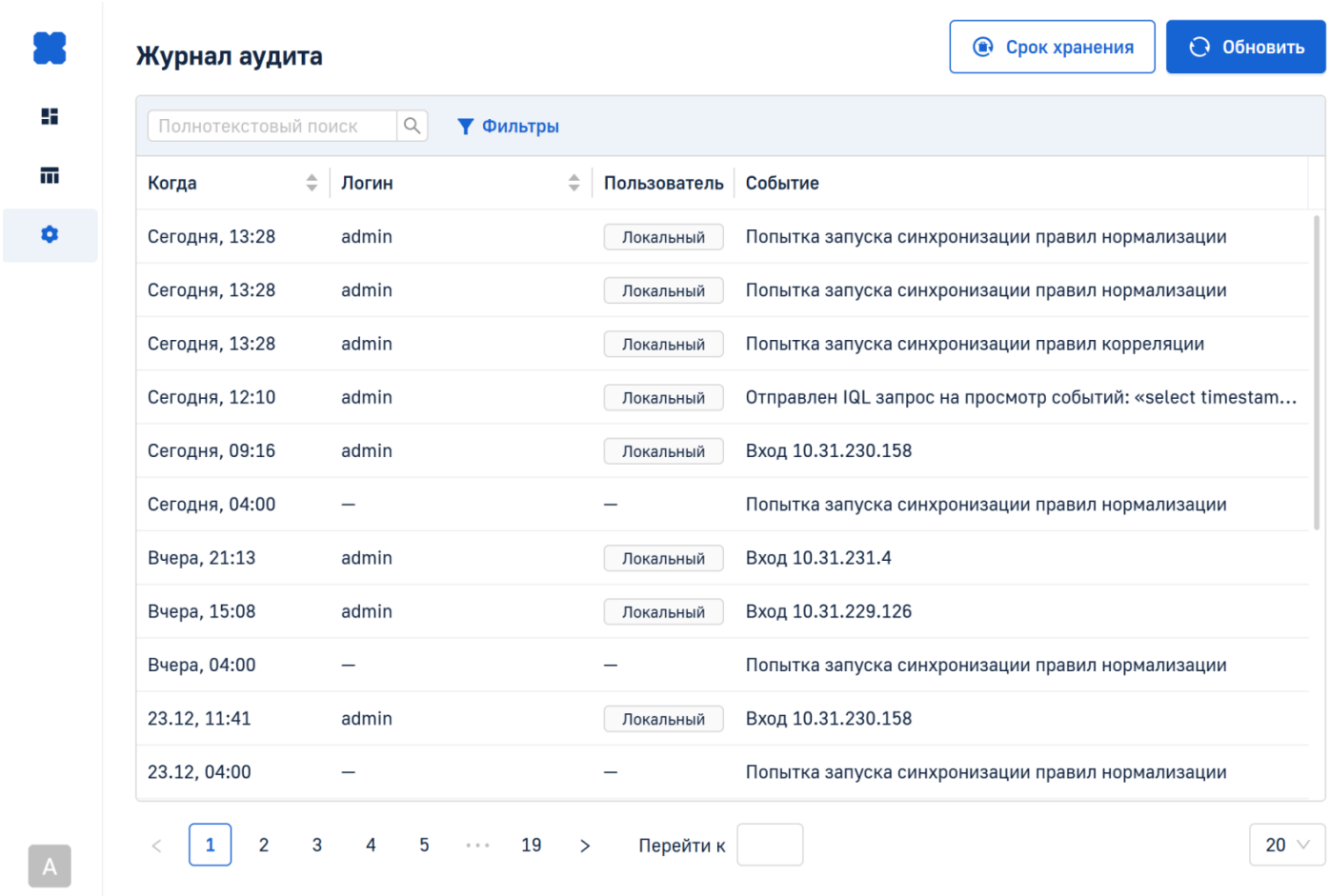
Просмотр и конфигурация журнала аудита

В данной статье описано взаимодействие с историей действий пользователей в Системе: как просмотреть и отфильтровать действия пользователей в Системе, а также описан процесс настройки длительности хранения записей в журнале.

Общие сведения

Для просмотра истории действий пользователей в Системе, необходимо перейти на страницу **Настройки → Журнал аудита**.



На данной странице отображается таблица со списком всех произведенных пользователями действий в различных разделах Системы:

- Дашборды:
  - Создан дашборд;
  - Переименован дашборд;
  - Удален дашборд;
  - Импортирован дашборд;
  - Экспортирован дашборд;
  - Доступ пользователя к дашборду предоставлен;
  - Доступ пользователя к дашборду отозван;
  - На дашборде создан виджет;
  - На дашборде изменен виджет;
  - С дашборда удален виджет;
  - На дашборд импортирован виджет;
  - С дашборда экспортирован виджет.

  События:
  - Скачаны события из тенанта;
  - Создан SQL-запрос;
  - Изменен SQL-запрос;
  - Удален SQL-запрос;
  - Создана папка SQL-запросов;
  - Изменена папка SQL-запросов;
  - Удалена папка SQL-запросов;
  - Отправлен запрос на просмотр событий.
- Тенанты:
  - Создан тенант;
  - Изменен тенант;
  - Удален тенант.
- Пользователи:
  - Авторизация пользователя;

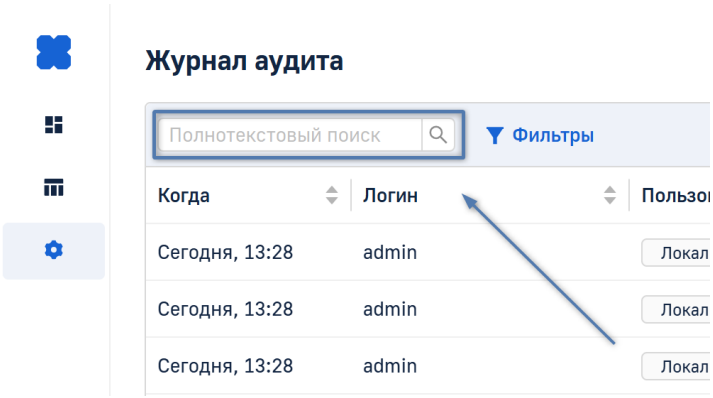
    - Неудачная попытка входа;
    - Окончание сессии пользователя;
    - Создан пользователь;
    - Изменены данные пользователя;
    - Удалён пользователь;
    - Заблокирован пользователь;
    - Разблокирован пользователь.
- Роли:
    - Создана роль;
    - Изменена роль;
    - Удалена роль;
    - Изменена роль по умолчанию.
- LDAP:
    - Изменены настройки LDAP-подключения.
- SMTP:
    - Изменены настройки SMTP-подключения.
- Компоненты системы:
    - Попытка запуска синхронизации правил корреляции;
    - Попытка запуска синхронизации правил нормализации.
- Конфигурационные файлы:
    - Загружен файл;
    - Загружена папка;
    - Скачан объект;
    - Создан файл;
    - Создана папка;
    - Удален файл;
    - Удалена папка;
    - Переименован файл.

Таблица содержит следующие поля:

- **Когда** — точная дата и время, когда было произведено то или иное действие;
- **Логин** — имя пользователя, совершившего то или иное действие;
- **Пользователь** — тип пользователя, совершившего то или иное действие;
- **Событие** — описание действия, которое произвел пользователь.

Поиск и фильтрация событий

Для того, чтобы найти определенного пользователя в списке, нажмите на форму поиска в левом верхнем углу таблицы и введите ключевое слово.



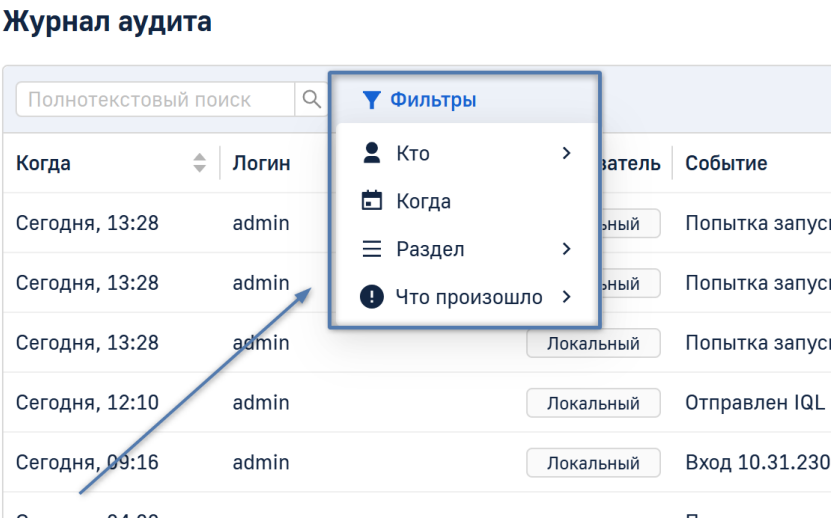
В качестве ключевых слов для поиска могут быть использованы:

- Имя пользователя;
- Текст события.

Вы также можете отфильтровать список событий по следующим параметрам:

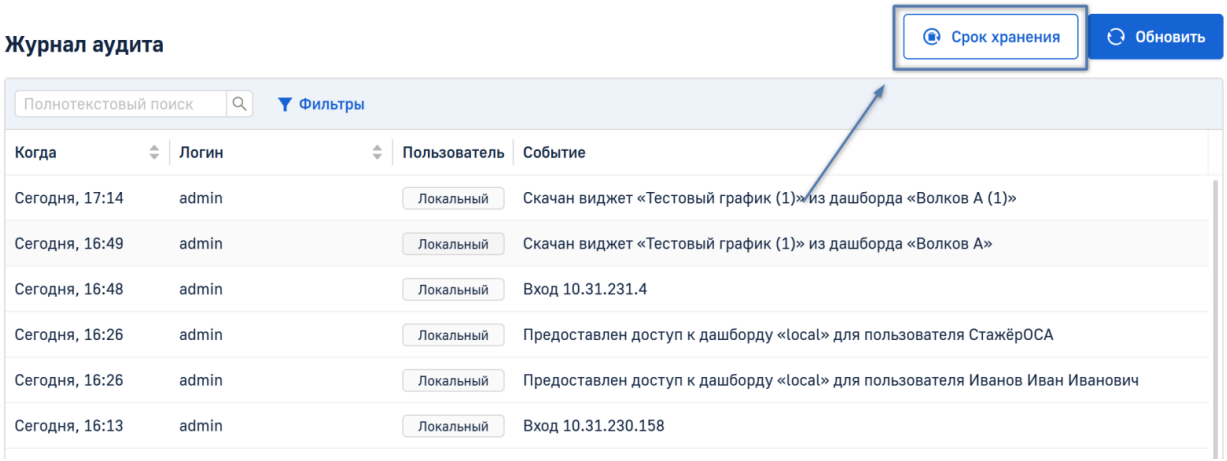
- **Кто** — фильтрация по пользователю, совершившему то или иное действие;
- **Когда** — фильтрация по дате и времени, когда было произведено то или иное действие;
- **Раздел** — фильтрация по разделу Системы, в котором было произведено то или иное действие;
- **Что произошло** — фильтрация по типу действия, совершенному в Системе.

Для этого нажмите на иконку фильтра и выберите параметры для фильтрации списка.



Конфигурация срока хранения действий в Системе

Для того, чтобы настроить срок хранения действий, сохраненных в Системе, нажмите **Срок хранения** в правом верхнем углу страницы. После этого укажите количество дней хранения. Все изменения будут применены автоматически. По умолчанию срок хранения действий — 180 дней.



Если вы хотите хранить действия бессрочно, активируйте переключатель **Бессрочно**.

ID статьи: 195
Последнее обновление: 28 дек., 2024
Обновлено от: Егоров В.
Ревизия: 5
База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.3.0 -> LogIQ. Руководство администратора -> Журнал аудита -> Просмотр и конфигурация журнала аудита
https://docs.axel.pro/entry/195/